

Rapport du Projet d'ingénierie ICCN INE2

Filière: Cybersécurité et Confiance Numérique

Sujet

Mise en place d'une infrastructure d'entreprise sécurisée
avec filtrage et détection d'anomalies par des techniques
de l'IA

Soutenu par :

LAOUIJ Hamza
BENTAJA Othmane
AIT KHOUYA Mohamed
BENNACEUR Oussama
AIT IZANA Ismail
SETTAF Ouafae

Sous la direction de :

Prof. AYACHE Meryeme
Prof. OUADDAH Aafaf
Prof. MEZRIOUI Abdellatif
Prof. BELMEKKI El Mostafa

Résumé

Les objectifs de ce projet sont multiples :

- Appliquer les connaissances et techniques apprises dans différents cours.
- Mettre en place une infrastructure réseau d'une entreprise avec ses services.
- Mettre en place des mesures de sécurité.

Pour atteindre ces objectifs, nous devons :

- Réaliser la maquette ci-dessous (figure 1), en salle TP, qui reflète le réseau d'une entreprise fictive (nommée sysco) reliée par un réseau public à une annexe régionale.
- Configurer les services réseaux demandés (figure 1)
- Mettre à la disposition de l'administrateur un outil de monitoring de la sécurité.

La conception de la maquette a été faite dans le sens de retrouver un environnement proche de celui d'une entreprise. La configuration d'une telle maquette nécessite le passage par plusieurs phases pour arriver enfin à une maquette sur laquelle plusieurs services fonctionnent en même temps.

La mise en place d'une telle maquette nécessite d'abord la préparation séparée des fichiers de configuration des différents services sur vos machines (machines virtuelles, GNS3, etc.) en suite l'accès à la salle TP pendant une demi-journée par semaine pour l'intégration de ces services et la mise en œuvre définitive de la maquette et son « test d'acceptation ».

Table des matières

Filière: Cybersécurité et Confiance Numérique.....	1
Résumé.....	3
Table des matières	5
Phase I	8
Mise en place de l'infrastructure et ses services	8
Mise en place de l'infrastructure et ses services	9
1.1 Plan d'adressage et routage	9
1.1.1 Plan d'adressage	9
1.1.2 Problème rencontré	9
1.1.3 Matrice de flux	10
1.1.4 Configuration du routeur	10
1.1.5 Configuration du Switch	12
1.1.6 Test de la configuration réseau.....	13
1.2 Configuration du NAT	14
1.2.1 Définition	14
1.2.2 Solution proposée pour le NAT	14
1.2.3 Configuration des routeurs	15
1.3 Configuration DHCP	15
1.4 Configuration DNS	18
1.4.1 Définition	18
1.4.2 Configuration du DNS	18
1.5 Configuration du Serveur WEB (Apache)	19
1.5.1 Définition	19
1.5.2 Configuration d'Appache	19
1.6 Configuration du serveur de messagerie (Postfix)	21
1.6.1 Configuration	21
1.6.2 Test d'envoi des mails :.....	25
1.7 Configuration WAF.....	26
1.8 Maquette de transition IPV4-6	27
Phase II.....	29
Sécurité du réseau.....	29
Sécurité du réseau.....	30

Table des matières

2.1 Configuration SQUID	30
2.1.1 Définition	30
2.1.2 Configuration	30
2.2 Configuration OPENLDAP	34
2.2.1 Définition	34
2.2.2 Configuration LDAP	34
2.3 Configuration Snort IDS	36
2.4 Configuration de Rsyslog	39
2.5 Configuration SIEM	40

Phase I

Mise en place de l'infrastructure et ses services

Au niveau de cette phase, nous devons :

- Etablir la connectique et élaborer un plan d'adressage
- Choisir une manière de faire le routage et le configurer
- Configurer le NAT éventuellement sur les routeurs
- Mettre en place les services réseaux : DHCP, DNS, MAIL, WEB, WAF, APPACHE, Maquette de transition IPV4-6

Mise en place de l'infrastructure et ses services

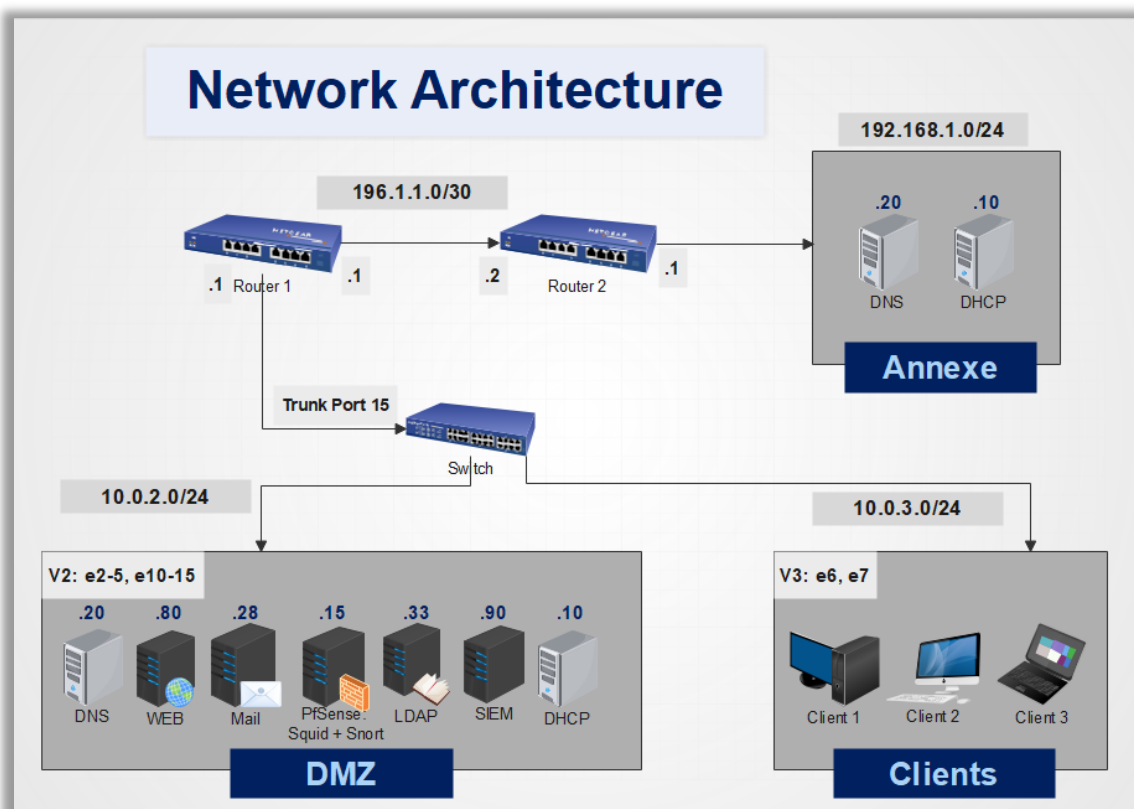
1.1 Plan d'adressage et routage

1.1.1 Plan d'adressage

Le réseau de notre entreprise est divisé en deux parties :

Siège : Contenant des adresses statiques pour les serveurs DNS interne, WEB, Mail, Pfsense (Squid), LDAP, SIEM, DHCP server et SNORT comme IDS dans le VLAN 2 (10.0.2.0/24) et un adressage dynamique pour les clients interne de l'entreprise dans le VLAN 3 (10.0.3.0/24).

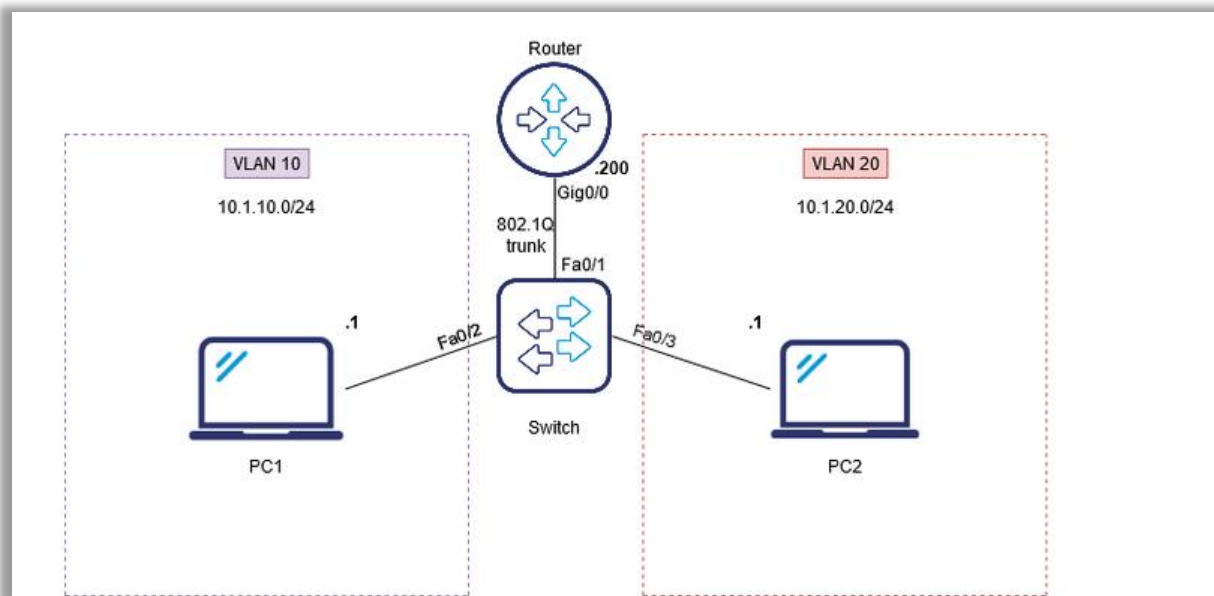
Annexe : Contenant le serveur DNS externe et le reste des employés de l'entreprise (192.168.1.0/24).



1.1.2 Problème rencontré

Lors du routage inter-vlan, on a trouvé que le switch est de niveau 3, ce qui ne nous permet pas de router les VLANs uniquement à travers le switch.

La solution proposée est l'utilisation d'une méthode appelée 'Router on Stick', expliquée dans le schéma ci-dessous :



1.1.3 Matrice de flux

	Siège	Annexe
Siège	<ul style="list-style-type: none"> - Permettre la communication entre les deux Vlan 	<ul style="list-style-type: none"> - Permit UDP 53 - Permit TCP 53 - Permit TCP 443 - Permit TCP 80 - Permit TCP 25
Annexe	<ul style="list-style-type: none"> - Permit UDP 53 - Permit TCP 53 - Permit TCP 443 - Permit TCP 80 	

1.1.4 Configuration du routeur

On a, donc, créé deux interfaces virtuelles (sub-interfaces Gigabit Ethernet 0/0.2 et 0/0.3) puis on a lié chaque interface avec un VLAN, pour ensuite router le trafic à travers l'interface logique Gigabit Ethernet 0/0.

Ensuite, on a configuré chaque interface avec son propre adressage :

```

interface GigabitEthernet0/0
description trunk link to switch
ip address 10.0.1.1 255.255.255.0
ip nat inside
ip virtual-reassembly
duplex auto
speed auto
ipv6 address 2001:CAFE:A:1::3/64
ipv6 address 2001:CAFE:A:1::/64 eui-64
ipv6 enable
!
interface GigabitEthernet0/0.2
description default gateway for vlan2
encapsulation dot1q 2
ip address 10.0.2.1 255.255.255.0
ip helper-address 10.0.2.10
ip nat inside
ip virtual-reassembly
!
interface GigabitEthernet0/0.3
description default gateway for vlan3
encapsulation dot1q 3
ip address 10.0.3.1 255.255.255.0
ip helper-address 10.0.2.10
ip nat inside
ip virtual-reassembly
.

```

```

interface Serial0/0/0
ip address 196.1.1.1 255.255.255.252
ip nat outside
ip virtual-reassembly
ipv6 address 2001:DB8:10:3::2/64
ipv6 rip rss enable
no fair-queue
no clock rate 2000000

```

Pour des raisons de test, on affiche la configuration des interfaces :

```

R3#show ip interf brief

```

Interface	IP-Address	OK?	Method	Status	Protocol
GigabitEthernet0/0	10.0.1.1	YES	manual	up	up
GigabitEthernet0/0.2	10.0.2.1	YES	NVRAM	up	up
GigabitEthernet0/0.3	10.0.3.1	YES	NVRAM	up	up
GigabitEthernet0/1	192.168.30.1	YES	NVRAM	down	down
Serial0/0/0	196.1.1.1	YES	NVRAM	up	up
Serial0/0/1	192.168.3.1	YES	NVRAM	down	down

Afin de router le trafic, on choisit le routage statique : On a, donc, créé une route par défaut au niveau des deux routeurs :

```

ip route 192.168.1.0 255.255.255.0 196.1.1.2
ip route 192.168.2.0 255.255.255.0 196.1.1.2
!

```

```

ip route 10.0.0.0 255.255.0.0 196.1.1.1
ip route 196.1.1.0 255.255.255.0 196.1.1.1
!

```

On affiche, maintenant, les routes :

```

R3#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default, U - per-user static route
        o - ODR, P - periodic downloaded static route, + - replicated route

Gateway of last resort is not set

10.0.0.0/8 is variably subnetted, 6 subnets, 2 masks
C       10.0.1.0/24 is directly connected, GigabitEthernet0/0
L       10.0.1.1/32 is directly connected, GigabitEthernet0/0
C       10.0.2.0/24 is directly connected, GigabitEthernet0/0.2
L       10.0.2.1/32 is directly connected, GigabitEthernet0/0.2
C       10.0.3.0/24 is directly connected, GigabitEthernet0/0.3
L       10.0.3.1/32 is directly connected, GigabitEthernet0/0.3
S       192.168.1.0/24 [1/0] via 196.1.1.2
S       192.168.2.0/24 [1/0] via 196.1.1.2
196.1.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       196.1.1.0/30 is directly connected, Serial0/0/0
L       196.1.1.1/32 is directly connected, Serial0/0/0

```

1.1.5 Configuration du Switch

On crée trois VLANs :

VLAN 2 : DMZ Interne avec un adressage 10.0.2.0/24

VLAN 3 : Pour les utilisateurs de l'entreprise avec un adressage 10.0.3.0/24

VLAN 15 : Pour le port trunk lié avec le routeur

```

switch# show vlan

Status and Counters - VLAN Information

Maximum VLANs to support : 8
Primary VLAN : LINKROUTER
Management VLAN :

802.1Q VLAN ID Name          Status          Voice
-----
1          LINKROUTER      Port-based      No
2          DMZ              Port-based      No
3          CLIENT           Port-based      No
15         VLAN15              Port-based      No

```

On configure, ensuite, change VLAN en ajoutant les ports :

Tagged : Port trunk relié avec le routeur.

Untagged : Port normal utilisé par les utilisateurs et les serveurs.

```

trunk 15 Trk1 LACP
ip default-gateway 10.0.1.1
snmp-server community "public" Unrestricted
vlan 1
    name "LINKROUTER"
    untagged 1,8-14,16-26,Trk1
    no ip address
    no untagged 2-7
    exit
vlan 2
    name "DMZ"
    untagged 2-5
    no ip address
    tagged 17,Trk1
    exit
vlan 3
    name "CLIENT"
    untagged 6-7
    no ip address
    tagged 17,Trk1
    exit
vlan 15
    name "VLAN15"
    tagged 17
    exit
spanning-tree Trk1 priority 4

```

1.1.6 Test de la configuration réseau

Enfin, on fait des tests de pings pour s'assurer que notre configuration fonctionne correctement :

Ping entre les deux routeurs :

```

R3#ping 196.1.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 196.1.1.1, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

```

Ping d'une machine en VLAN 2 vers la passerelle :

```

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . : Sysco.ma
    IPv6 Address. . . . . : fd92:a19a:c377::a27
    Link-local IPv6 Address . . . . . : fe80::88a4:8ef2:d0fb:c1b2%11
    IPv4 Address. . . . . : 10.0.2.11
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.0.2.1

```

```
C:\Users\Hamza>ping 10.0.2.1

Pinging 10.0.2.1 with 32 bytes of data:
Reply from 10.0.2.1: bytes=32 time<1ms TTL=255
Reply from 10.0.2.1: bytes=32 time<1ms TTL=255
Reply from 10.0.2.1: bytes=32 time<1ms TTL=255
Reply from 10.0.2.1: bytes=32 time<1ms TTL=255

Ping statistics for 10.0.2.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Ping d'une machine en VLAN 2 vers la passerelle du VLAN 3 :

```
C:\Users\Hamza>ping 10.0.3.1

Pinging 10.0.3.1 with 32 bytes of data:
Reply from 10.0.3.1: bytes=32 time<1ms TTL=255
Reply from 10.0.3.1: bytes=32 time<1ms TTL=255
Reply from 10.0.3.1: bytes=32 time<1ms TTL=255
Reply from 10.0.3.1: bytes=32 time=1ms TTL=255

Ping statistics for 10.0.3.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Ping d'une machine en VLAN 2 vers une machine en VLAN 3 :

```
C:\Users\Hamza>ping 10.0.3.14

Pinging 10.0.3.14 with 32 bytes of data:
Reply from 10.0.3.14: bytes=32 time<1ms TTL=63
Reply from 10.0.3.14: bytes=32 time<1ms TTL=63
Reply from 10.0.3.14: bytes=32 time=1ms TTL=63
Reply from 10.0.3.14: bytes=32 time=1ms TTL=63

Ping statistics for 10.0.3.14:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

1.2 Configuration du NAT

1.2.1 Définition

Le Network Address Translation désigne un mécanisme de virtualisation d'adresses IP qui permet de traduire ou de convertir des adresses IP en d'autres adresses IP. Le mécanisme contribue à améliorer la sécurité et à diminuer le nombre d'adresses IP nécessaires à une entreprise.

1.2.2 Solution proposée pour le NAT

- **NAT Statique** : Afin de permettre aux serveurs d'avoir une adresse statique et, ainsi, être joignable à n'importe quel moment.
- **NAT Overload** : Pour permettre aux utilisateurs de l'entreprise d'accéder à internet

avec un minimum d'adresses publiques en utilisant les ports.

1.2.3 Configuration des routeurs

1.2.3.1 Routeur 1 :

D'abord, on définit les interface IN (Gigabit Ethernet 0/0) et les interfaces OUT (Serial 0/0/0) :

```
interface GigabitEthernet0/0
description trunk link to switch
ip address 10.0.1.1 255.255.255.0
ip nat inside
ip virtual-reassembly
duplex auto
speed auto
ipv6 address 2001:CAFE:A:1::3/64
ipv6 address 2001:CAFE:A:1::/64 eui-64
ipv6 enable
```

```
interface Serial0/0/0
ip address 196.1.1.1 255.255.255.252
ip nat outside
ip virtual-reassembly
ipv6 address 2001:DB8:10:3::2/64
ipv6 rip rss enable
no fair-queue
no clock rate 2000000
```

Ensuite, comme mentionné sur la figure d'architecture réseau, chaque serveur a une adresse publique statique (à partir de la 2^{ème} ligne), alors que les utilisateurs ont un NAT Overload (1^{ère} ligne).

```
ip nat inside source list 1 interface Serial0/0/0 overload
ip nat inside source static 10.0.2.15 196.1.1.15
ip nat inside source static 10.0.2.28 196.1.1.28
ip nat inside source static 10.0.2.33 196.1.1.33
ip nat inside source static 10.0.2.80 196.1.1.80
ip nat inside source static 10.0.2.90 196.1.1.90
```

1.2.3.2 Routeur 2 :

De même pour le routeur de l'annexe, on a opté pour la même solution :

```
ip nat inside source list 1 interface Serial0/0/0 overload
ip nat inside source static 192.168.1.20 196.1.1.20
```

1.3 Configuration DHCP

Vu la complexité de l'architecture réseau au niveau du siège, on a implémenté un DHCP server sur une machine linux. Cependant, au niveau de l'annexe on choisit de configurer DHCP directement sur le routeur.

1.3.1.1 DHCP Server pour le siège

Après installation des packages DHCP, on configure notre serveur à l'aide du fichier

‘/etc/dhcp/dhcpd.conf’

```
GNU nano 2.3.1      File: /etc/dhcp/dhcpd.conf

option domain-name "Sysco.ma";
option domain-name-servers 10.0.2.85;
default-lease-time 600;
max-lease-time 7200;

authoritative;
log-facility local7;

## VLAN 2 Pool
subnet 10.0.2.0 netmask 255.255.255.0 {
    range 10.0.2.10 10.0.2.254;
    option routers 10.0.2.1;
    option broadcast-address 10.0.2.255;
}

## VLAN 3 Pool
subnet 10.0.3.0 netmask 255.255.255.0 {
    range 10.0.3.10 10.0.3.254;
    option routers 10.0.3.1;
    option broadcast-address 10.0.3.255;
}
```

Option domain-name : Le nom de domaine de notre entreprise.

Option domain-name-servers : L'adresse IP du serveur DNS de l'entreprise.

Default-lease-time : La durée par défaut pour garder une adresse IP.

Max-lease-time : La durée maximale pour garder une adresse IP.

Authoritative : Ce serveur DHCP est le seul qui distribue les adresses dans ce réseau.

Log-facility : Activation de l'envoi des logs au serveur rsyslog.

Afin de garantir que chaque serveur aie une adresse IP statique, on configure notre serveur :

```
host WEB {
    hardware ethernet 00:0C:29:AF:3C:A4;
    fixed-address 10.0.2.80;
}

host MAIL {
    hardware ethernet 08:00:27:3C:A0:DC;
    fixed-address 10.0.2.28;
}

host DNS {
    hardware ethernet 00:0c:29:75:74:3e;
    fixed-address 10.0.2.85;
}
```



```
host rsyslog {
    hardware ethernet 00:0C:29:60:2A:0E;
    fixed-address 10.0.2.90;
}

host PfSense {
    hardware ethernet 08:00:27:14:CE:32;
    fixed-address 10.0.2.15;
}

host LDAP {
    hardware ethernet 08:00:27:DB:6D:25;
    fixed-address 10.0.2.33;
}

host SQUID {
    hardware ethernet 08:0C:29:1A:2C:85;
    fixed-address 10.0.2.25;
}
```

Host : Nom de la machine hôte.

Hardware ethernet : Adresse MAC de la machine.

Fixed-address : Adresse IP fixe.

Ce serveur distribuera les adresses pour les deux VLANS en même temps. Pour cela, on doit configurer un relai au niveau du routeur (ip helper-address ip_dhcp_server):

```
interface GigabitEthernet0/0.2
description default gateway for vlan2
encapsulation dot1q 2
ip address 10.0.2.1 255.255.255.0
ip helper-address 10.0.2.10
ip nat inside
ip virtual-reassembly
!
interface GigabitEthernet0/0.3
description default gateway for vlan3
encapsulation dot1q 3
ip address 10.0.3.1 255.255.255.0
ip helper-address 10.0.2.10
ip nat inside
ip virtual-reassembly
```

1.3.1.2 DHCP au niveau du routeur pour l'annexe

La configuration du DHCP au niveau du routeur passe par les étapes suivantes :

- Déclaration des adresses exclus :

```
ip dhcp excluded-address 192.168.1.1 192.168.1.10
!
```

- Déclaration d'une pool d'adresses :
Dans cette pool, on déclare aussi la passerelle, l'adresse IP du DNS Server et le nom de domaine.

```
ip dhcp pool annexe
network 192.168.1.0 255.255.255.0
default-router 192.168.1.1
dns-server 192.168.1.20
domain-name Sysco.ma
```

- Adressage statique pour le DNS Server :

```
ip dhcp pool dnsserver
host 192.168.1.20 255.255.255.0
hardware-address 0800.27b3.a834
!
```

1.4 Configuration DNS

1.4.1 Définition

Le serveur DNS (Domain Name System) est un service dont la principale fonction est de traduire un nom de domaine en adresse IP. Pour simplifier, le serveur DNS agit comme un annuaire que consulte un ordinateur au moment d'accéder à un autre ordinateur via un réseau.

1.4.2 Configuration du DNS

Pour la configuration du DNS on a implémenté deux serveur DNS, un interne et l'autre externe (dans l'annexe).

Après installation des packages DNS, on configure notre serveur à l'aide du fichier '/etc/named.conf' :

```
//
// named.conf
//
// Provided by Red Hat bind package to configure the ISC BIND named(8) DNS
// server as a caching only nameserver (as a localhost DNS resolver only).
//
// See /usr/share/doc/bind*/sample/ for example named configuration files.
//
// See the BIND Administrator's Reference Manual (ARM) for details about the
// configuration located in /usr/share/doc/bind-{version}/Bv9ARM.html

options {
    listen-on port 53 { 10.0.2.0/24,10.0.3.0/24; };
    listen-on-v6 port 53 { ::1; };
    directory "/var/named";
    allow-query { 10.0.2.0/24,10.0.3.0/24; };
};
zone "." IN {
    type hint;
    file "named.ca";
};
zone "Sysco.ma" IN {
    type master;
    file "mysite.db";
};
zone "2.0.10.in-addr.arpa" IN {
    type master;
    file "1.168.192.db";
};
```

Lors de notre configuration du DNS, on a laissé passer les requêtes DNS par le Réseau VLAN 2 (10.0.2.0/24) et VLAN 3 (10.0.3.0/24).

On fait un test avec la commande nslookup :

```
[root@dnsserver okio]# nslookup
> www.sysco.ma
Server:      10.0.2.85
Address:     10.0.2.85#53

Name:   www.Sysco.ma
Address: 10.0.2.80
> mail.sysco.ma
Server:      10.0.2.85
Address:     10.0.2.85#53

Name:   mail.Sysco.ma
Address: 10.0.2.28
```

On fait un test du ping vers le serveur web et le serveur mail :

```
[root@selcentos1 okio]# ping www.sysco.ma
PING www.Sysco.ma (10.0.2.80) 56(84) bytes of data.
64 bytes from www.Sysco.ma (10.0.2.80): icmp_seq=1 ttl=64 time=1.70 ms
64 bytes from www.Sysco.ma (10.0.2.80): icmp_seq=2 ttl=64 time=2.06 ms
^C
--- www.Sysco.ma ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1005ms
rtt min/avg/max/mdev = 1.700/1.881/2.063/0.186 ms
[root@selcentos1 okio]# ping mail.sysco.ma
PING mail.Sysco.ma (10.0.2.28) 56(84) bytes of data.
64 bytes from mail.Sysco.ma (10.0.2.28): icmp_seq=1 ttl=64 time=2.49 ms
64 bytes from mail.Sysco.ma (10.0.2.28): icmp_seq=2 ttl=64 time=1.67 ms
^C
--- mail.Sysco.ma ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1003ms
rtt min/avg/max/mdev = 1.671/2.085/2.499/0.414 ms
[root@selcentos1 okio]#
```

On a fait de même pour le DNS externe, on a seulement changé les adresses privées par des adresses publiques traduites par le NAT.

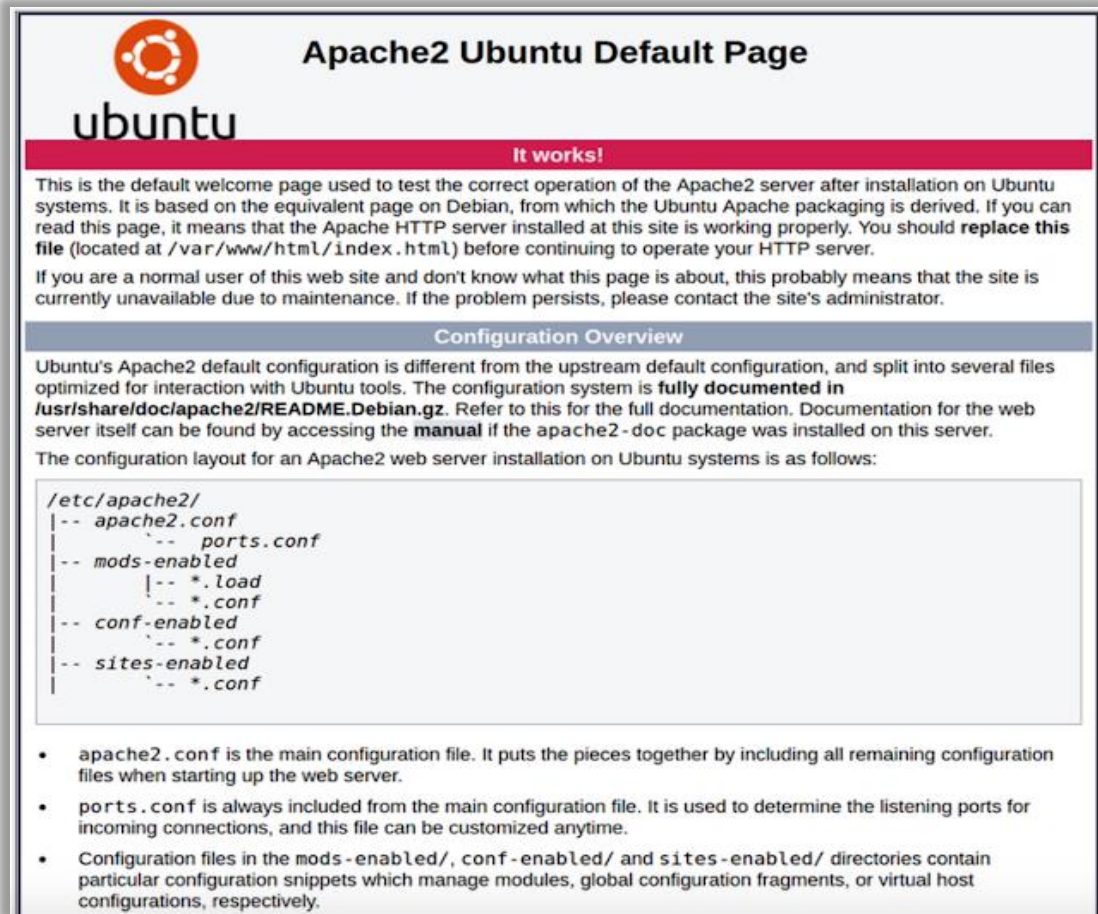
1.5 Configuration du Serveur WEB (Apache)

1.5.1 Définition

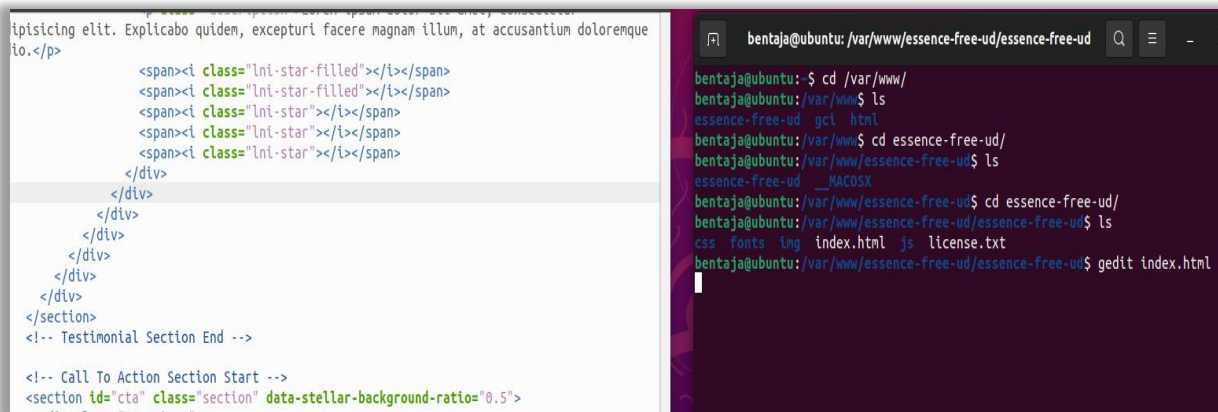
Le logiciel libre Apache HTTP Server est un serveur HTTP créé et maintenu au sein de la fondation Apache.

1.5.2 Configuration d'Apache

On installe les packages nécessaires pour configurer notre serveur Apache.



Ensuite, on crée notre site web

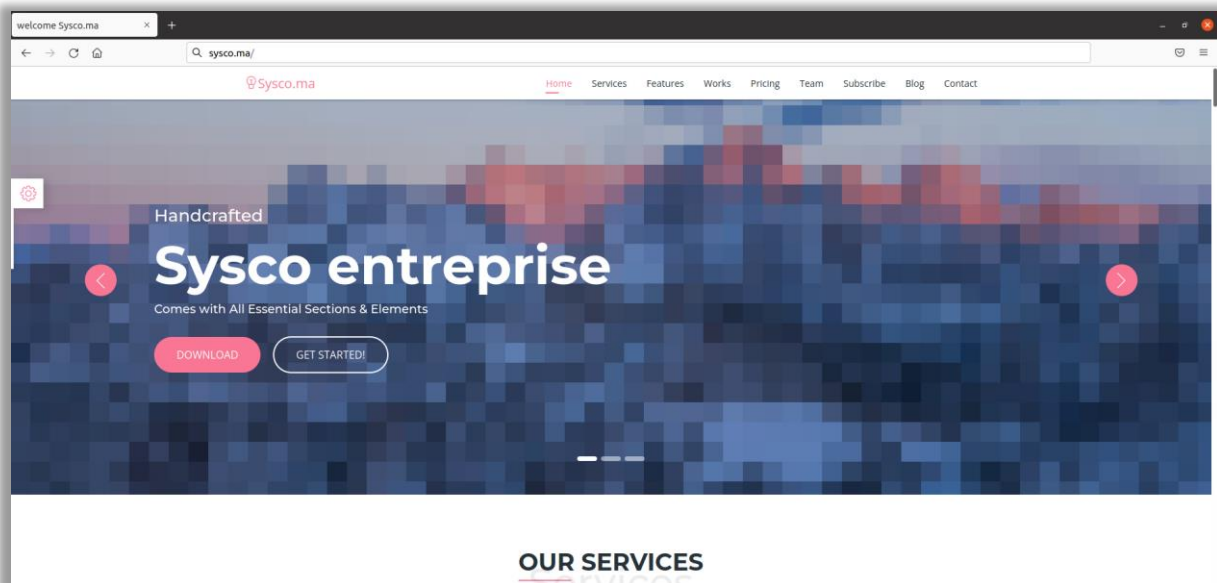


```
tualHost *:80>
# The ServerName directive sets the request scheme, hostname and port that
# the server uses to identify itself. This is used when creating
# redirection URLs. In the context of virtual hosts, the ServerName
# specifies what hostname must appear in the request's Host: header to
# match this virtual host. For the default virtual host (this file) this
# value is not decisive as it is used as a last resort host regardless.
# However, you must set it for any further virtual host explicitly.
#ServerName www.example.com

ServerAdmin otnanbentaja2@gmail.com
DocumentRoot /var/www/essence-free-ud/essence-free-ud/
ServerName www.sysco.ma

# Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
# error, crit, alert, emerg.
# It is also possible to configure the loglevel for particular
# modules, e.g.
#LogLevel info ssl:warn
```

On accède, maintenant, à notre site web depuis le navigateur



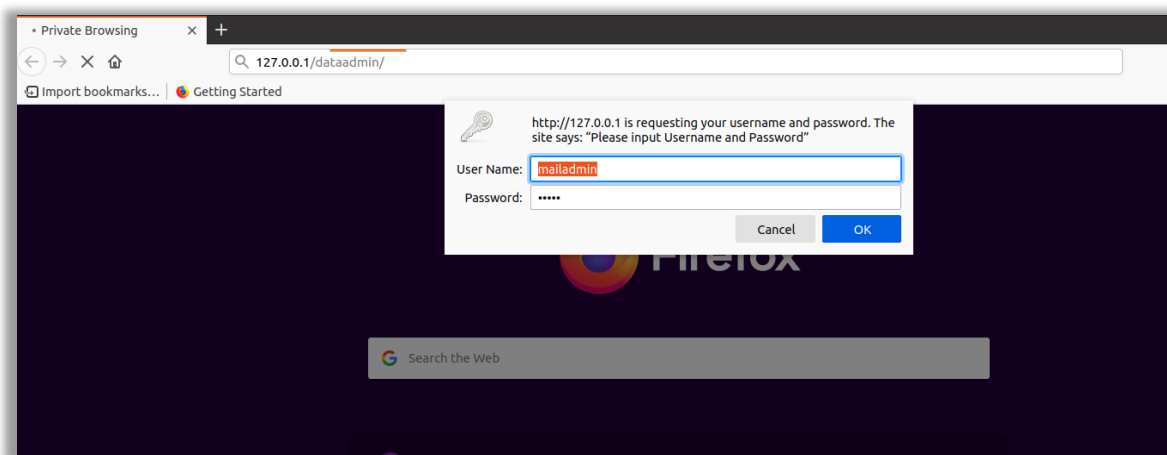
1.6 Configuration du serveur de messagerie (Postfix)

1.6.1 Configuration

D'abord on a installé PHPMYAdmin pour la création d'une base de données pour le serveur mail. Comme PHPMYAdmin est une cible pour les attaquants, on a sécurisé l'accès à cette interface et l'un des moyens les plus simples consiste à ajouter une passerelle devant l'ensemble de l'application PhpMyAdmin.

Pour ce faire, on utilise les fonctions d'authentification et d'authentification Apache intégrées. De plus, cela nécessite de modifier le fichier de configuration Apache pour lui permettre d'utiliser les remplacements de fichier `.htaccess`.

De plus, on a changé le path par défaut pour accéder à l'interface de login qui était /phpmyadmin avec un nom qui est un peu difficile à trouver au cas où l'attaquant a utilisé des outils de directory fuzzing.



Notre base de données est de la forme suivante :

Table	Action	Rows	Type	Collation	Size	Overhead
virtual_Allies	Browse Structure Search Insert Empty Drop	1	InnoDB	utf8_general_ci	48.0 KiB	-
virtual_Domains	Browse Structure Search Insert Empty Drop	1	InnoDB	utf8_general_ci	32.0 KiB	-
virtual_Status	Browse Structure Search Insert Empty Drop	1	InnoDB	utf8_general_ci	16.0 KiB	-
virtual_Users	Browse Structure Search Insert Empty Drop	4	InnoDB	utf8_general_ci	48.0 KiB	-
4 tables	Sum	7	InnoDB	utf8mb4_general_ci	144.8 KiB	0 B

Ensuite, on a installé Postfix avec ses dépendances et dans le fichier de configuration, on a ajouté notre domaine.

On change le banner par défaut qui s'affiche au cas où quelqu'un essaie de se connecter à notre serveur mail avec telnet, pour éviter toute forme d'une "information disclosure"

```
root@mail:~# telnet localhost 25
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
220 Sysco.ma hello this is our mail (sysco)
```

Et voici notre fichier de configuration final après avoir ajouté les locations des fichiers pour la connexion à la base de données déjà créée.


```

1 # See /usr/share/postfix/main.cf.dist for a commented, more complete version
2
3 # Debian specific: Specifying a file name will cause the first
4 # line of that file to be used as the name. The Debian default
5 # is /etc/mailname.
6 #myorigin = /etc/mailname
7
8 smtpd_banner = $myhostname hello this is our $mail_name (sysco)
9 biff = no
10
11 # appending .domain is the MUA's job.
12 append_dot_mydomain = no
13
14 # Uncomment the next line to generate "delayed mail" warnings
15 #delay_warning_time = 4h
16
17 readme_directory = no
18
19 # See http://www.postfix.org/COMPATIBILITY_README.html -- default to 2 on
20 # fresh installs.
21 compatibility_level = 2
22
23 ###Enabling SMTP for authenticated users, and handing off authentication to Dovecot
24
25 smtpd_sasl_type = dovecot
26 smtpd_sasl_path = private/auth
27 smtpd_sasl_auth_enable = yes
28
29 smtpd_sasl_auth_enable = yes
30
31 broken_sasl_auth_clients = yes
32
33 smtpd_sasl_authenticated_header = yes
34
35 virtual_transport = lmtp:unix:private/dovecot-lmtp
36
37 # See /usr/share/doc/postfix/TLS_README.gz in the postfix-doc package for
38 # information on enabling SSL in the smtp client.

```

```

inet_protocols = ipv4

# Handing off local delivery to Dovecot's LMTP, and telling it where to store mail
virtual_transport = lmtp:unix:private/dovecot-lmtp

# Virtual domains, users, and aliases
# These files contain the connection information for the MySQL lookup tables created in the
MySQL in the Part 2
virtual_mailbox_domains = mysql:/etc/postfix/virtual-domains.cf
virtual_mailbox_maps = mysql:/etc/postfix/virtual-users.cf
virtual_alias_maps = mysql:/etc/postfix/virtual-aliases.cf,
mysql:/etc/postfix/virtual-email2email.cf

# Even more Restrictions and MTA params
disable_vrfy_command = yes
strict_rfc821_envelopes = yes
#smtpd_etrn_restrictions = reject
#smtpd_reject_unlisted_sender = yes
#smtpd_reject_unlisted_recipient = yes
smtpd_delay_reject = yes
smtpd_helo_required = yes
smtp_always_send_ehlo = yes
#smtpd_hard_error_limit = 1
smtpd_timeout = 30s
smtp_helo_timeout = 15s
smtp_rcpt_timeout = 15s
smtpd_recipient_limit = 40
minimal_backoff_time = 180s
maximal_backoff_time = 3h

# Reply Rejection Codes
invalid_hostname_reject_code = 550
non_fqdn_reject_code = 550
unknown_address_reject_code = 550
unknown_client_reject_code = 550
unknown_hostname_reject_code = 550
unverified_recipient_reject_code = 550
unverified_sender_reject_code = 550

```

Après avoir configuré avec succès le Postfix, on a utilisé le Dovecot qui est un open source IMAP et POP3 serveur

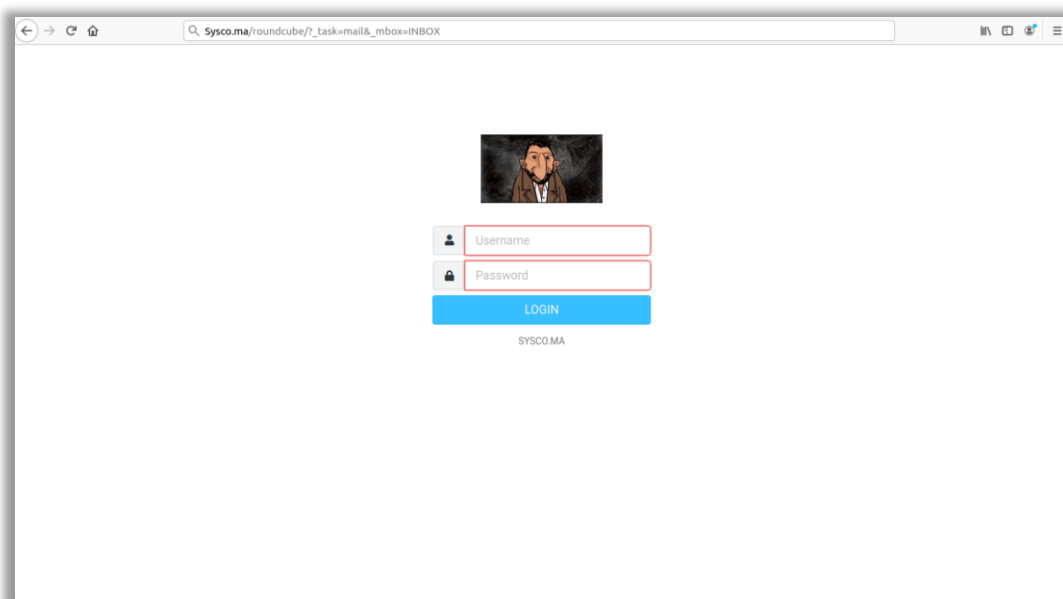
On a modifié son fichier de configuration pour qu'il puisse supporter les protocoles imap et pop3 et lmtp

```
13 # source/destination IPs by placing the settings inside sections, for example:
14 # protocol imap ( ), local 127.0.0.1 ( ), remote 10.0.0.0/8 ( )
15
16 # Default values are shown for each setting, it's not required to uncomment
17 # those. These are exceptions to this though: No sections (e.g. namespace {})
18 # or plugin settings are added by default, they're listed only as examples.
19 # Paths are also just examples with the real defaults being based on configure
20 # options. The paths listed here are for configure --prefix=/usr
21 # --sysconfdir=/etc --localstatedir=/var
22
23 # Enable installed protocols
24 !include_try /usr/share/dovecot/protocols.d/*.protocol
25 protocols = imap pop3 lmtp
26 # A comma separated list of IPs or hosts where to listen in for connections.
27 # "*" listens in all IPv4 interfaces, "::" listens in all IPv6 interfaces.
28 # If you want to specify non-default ports or anything more complex,
29 # edit conf.d/master.conf.
30 #listen = *, ::
31
32 # Base directory where to store runtime data.
33 #base_dir = /var/run/dovecot/
```

De même, il faut le connecter aussi à la base de donnée déjà créée

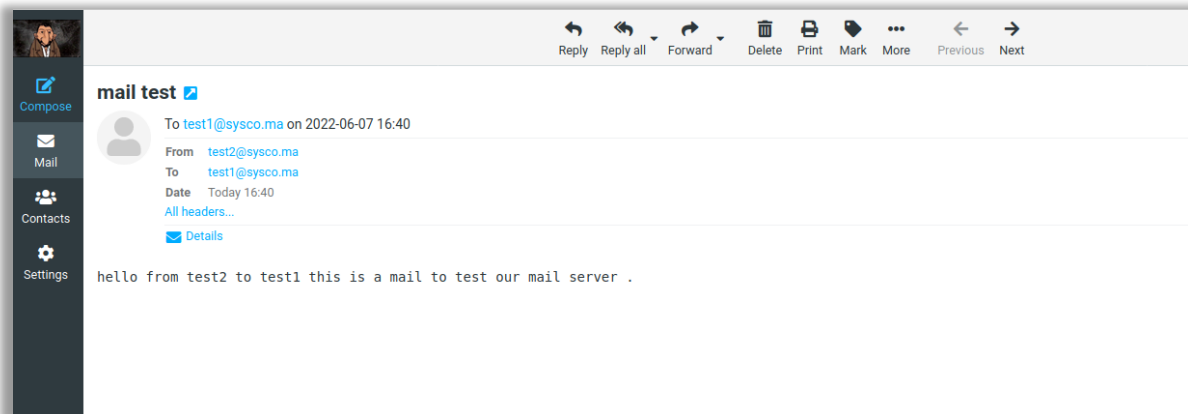
Pour monter le RoundCube, nous avons créé sa propre base de donnée et on a installé les extensions php qui sont indispensables pour la configuration de RoundCube, puis on a associé le RoundCube directory dans /var/www au user www-data pour qu'il sera limité en terme de privilèges au cas d'une intrusion.

Et voici notre interface de login

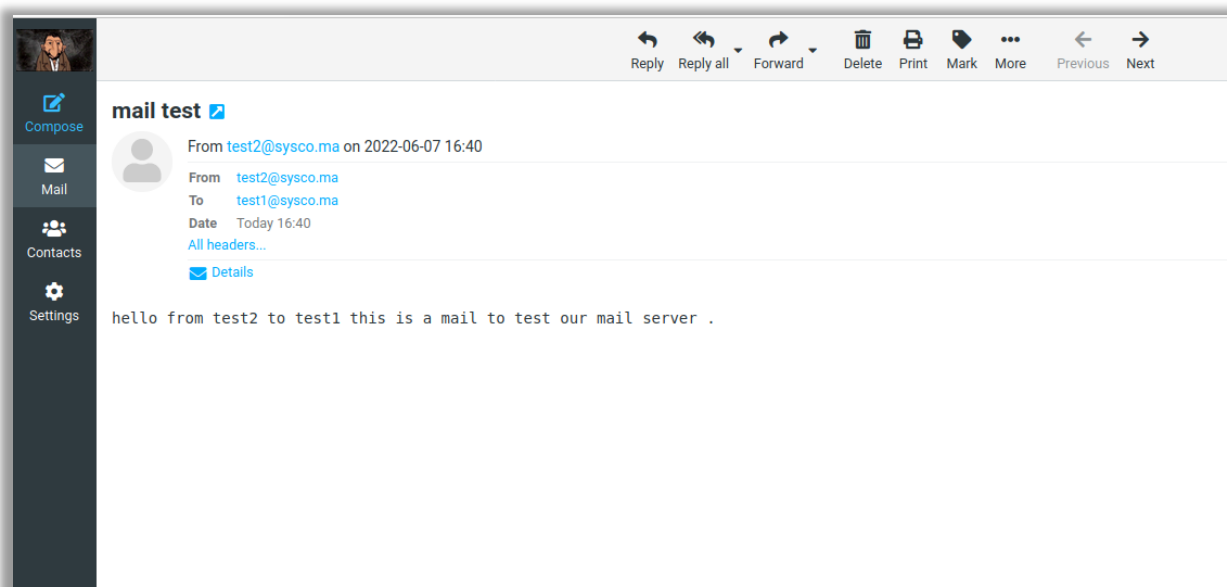
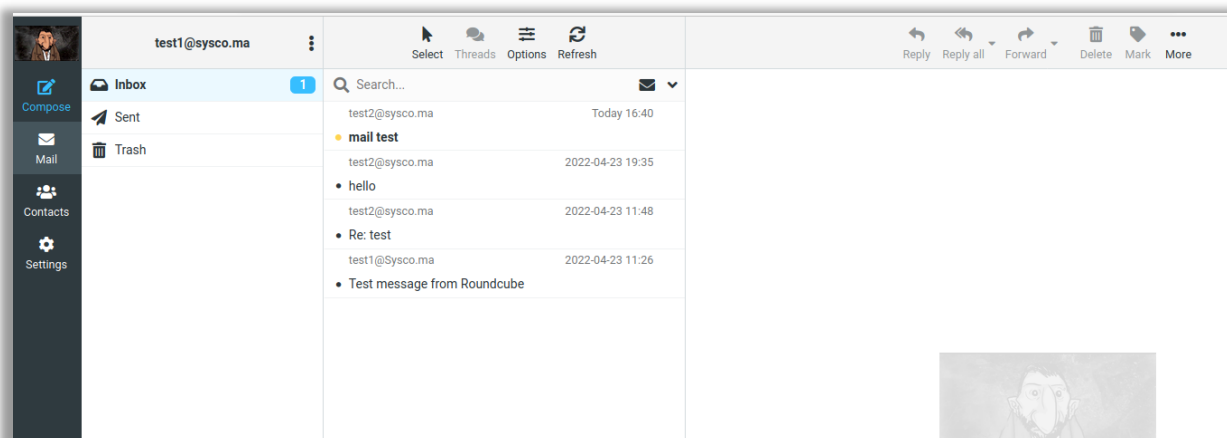


1.6.2 Test d'envoi des mails :

On a envoyé un mail à partir d'un utilisateur test1 à test2 :



Une notification sera affiché dans le compte de test2 :

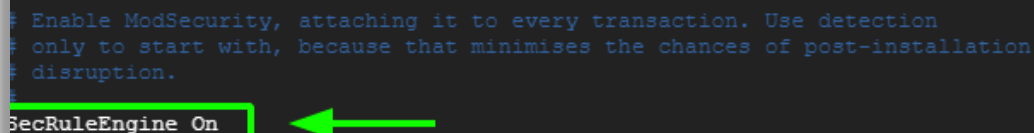


1.7 Configuration WAF

Pour la solution WAF, on a opté pour le modsecurity WAF qui est un projet open source

On a installé le package modsecurity. Par default, modsecurity est configuré pour la détection seulement des attaques et les afficher, c'est pour cela qu'il faut modifier son fichier de configuration `/etc/modsecurity/modsecurity.conf` et ajouter la ligne suivante

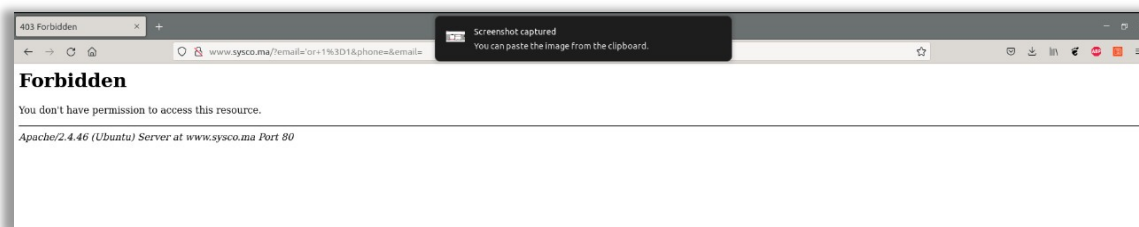
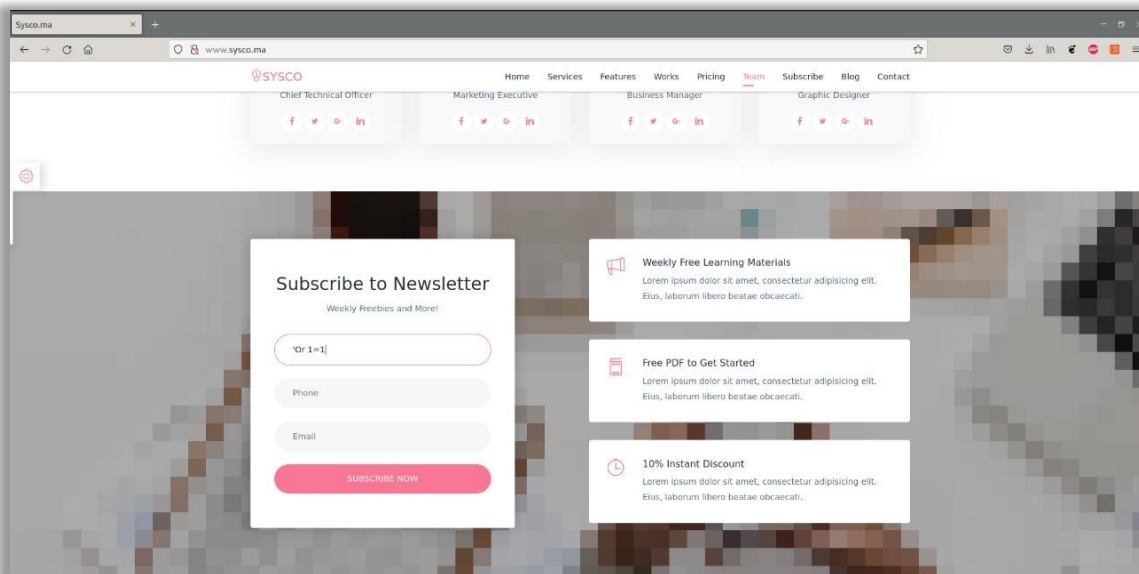
`SecRuleEngine DetectionOnly.`



```
# Enable ModSecurity, attaching it to every transaction. Use detection
# only to start with, because that minimises the chances of post-installation
# disruption.
SecRuleEngine On
```

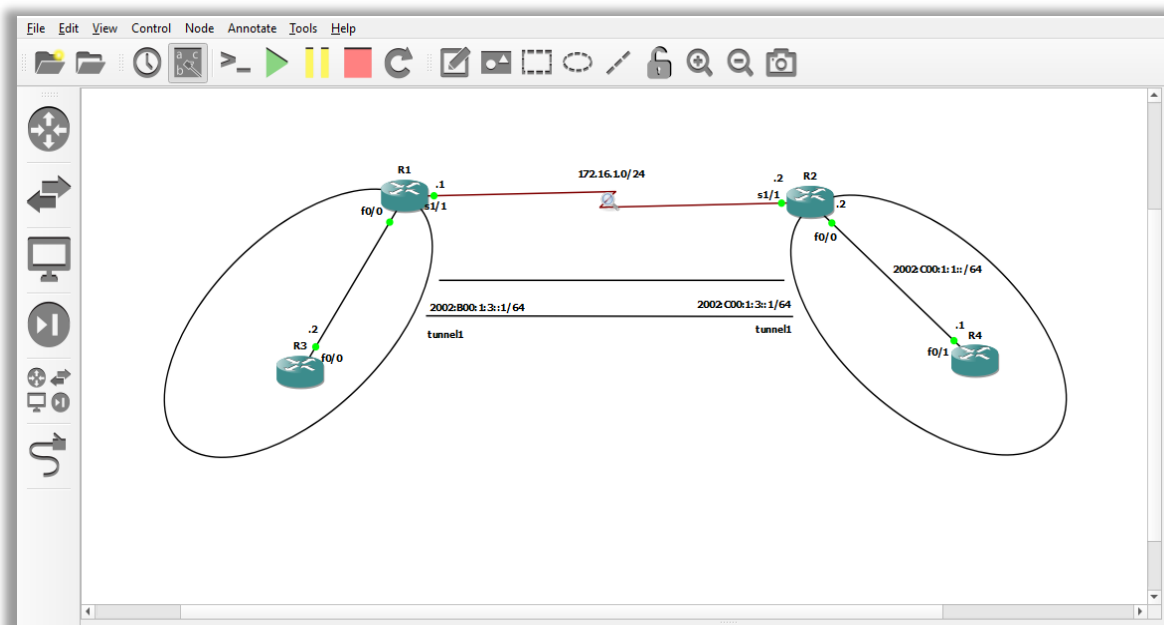
Après on a téléchargé OWASP ModSecurity Core Ruleset dans le dossier des fichiers de configuration de modsecurity, on a fait ces modifications dans le serveur mail, ainsi que pour le serveur web de mail (RoundCube).

Et pour tester notre configuration, il suffit d'envoyer un payload et on serait dirigé vers une page d'error.



1.8 Maquette de transition IPV4-6

Dans cette partie, on établit la maquette du TP du transition ipv6/ipv4, on a choisi le mode 6to4 pour effectuer la transition.



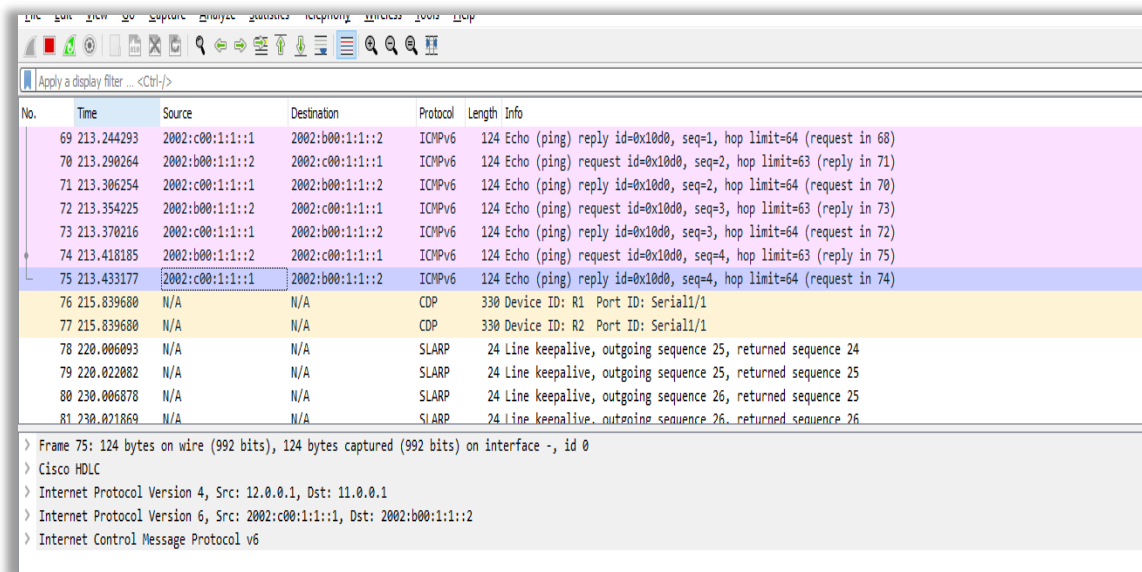
Après avoir configuré les routeurs, une capture a été lancée entre les routeurs R1 et R2 pour voir si le ping entre les interfaces du routeur R3 et celles du routeur R4 fonctionne.

```

R3#
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2002:C00:1:1::1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 52/64/72 ms
R3#
R3#
R3#
R3#
R3#
R3#
R3#
R3#
R3#ping 2002:c00:1:1::1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2002:C00:1:1::1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 56/58/60 ms
R3#

```

Le ping fonctionne bien, on vérifie maintenant la capture lancée :



Apply a display filter ... <Ctrl-F>

No.	Time	Source	Destination	Protocol	Length	Info
69	213.244293	2002:c00:1:1::1	2002:b00:1:1::2	ICMPv6	124	Echo (ping) reply id=0x10d0, seq=1, hop limit=64 (request in 68)
70	213.290264	2002:b00:1:1::2	2002:c00:1:1::1	ICMPv6	124	Echo (ping) request id=0x10d0, seq=2, hop limit=63 (reply in 71)
71	213.306254	2002:c00:1:1::1	2002:b00:1:1::2	ICMPv6	124	Echo (ping) reply id=0x10d0, seq=2, hop limit=64 (request in 70)
72	213.354225	2002:b00:1:1::2	2002:c00:1:1::1	ICMPv6	124	Echo (ping) request id=0x10d0, seq=3, hop limit=63 (reply in 73)
73	213.370216	2002:c00:1:1::1	2002:b00:1:1::2	ICMPv6	124	Echo (ping) reply id=0x10d0, seq=3, hop limit=64 (request in 72)
74	213.418185	2002:b00:1:1::2	2002:c00:1:1::1	ICMPv6	124	Echo (ping) request id=0x10d0, seq=4, hop limit=63 (reply in 75)
75	213.433177	2002:c00:1:1::1	2002:b00:1:1::2	ICMPv6	124	Echo (ping) reply id=0x10d0, seq=4, hop limit=64 (request in 74)
76	215.839680	N/A	N/A	CDP	330	Device ID: R1 Port ID: Serial1/1
77	215.839680	N/A	N/A	CDP	330	Device ID: R2 Port ID: Serial1/1
78	220.006093	N/A	N/A	SLARP	24	Line keepalive, outgoing sequence 25, returned sequence 24
79	220.022082	N/A	N/A	SLARP	24	Line keepalive, outgoing sequence 25, returned sequence 25
80	230.006878	N/A	N/A	SLARP	24	Line keepalive, outgoing sequence 26, returned sequence 25
81	230.021869	N/A	N/A	SLARP	24	Line keepalive, outgoing sequence 26, returned sequence 26

> Frame 75: 124 bytes on wire (992 bits), 124 bytes captured (992 bits) on interface -, id 0

> Cisco HDLC

> Internet Protocol Version 4, Src: 12.0.0.1, Dst: 11.0.0.1

> Internet Protocol Version 6, Src: 2002:c00:1:1::1, Dst: 2002:b00:1:1::2

> Internet Control Message Protocol v6

Phase II

Sécurité du réseau

Dans cette phase, nous attaquons les points suivants :

- Installer et configurer le serveur proxy SQUID pour permettre aux utilisateurs d'accéder à l'extérieur du site siège selon leur profil.
- Pour appliquer cette politique d'accès à tous les utilisateurs, nous aurons besoin d'installer et configurer un annuaire (OpenLDAP).
- Installer et mettre en place l'IDS Snort pour détecter les intrusions. Choisir l'emplacement adéquat.
- Tester le serveur IDS en utilisant des outils de scan et d'attaque réseau tel que nmap, nessus et autres.
- Une collecte des logs doit être mise en place et centralisée via rsyslog (logs du routeur, SQUID, IDS, etc). Ces données collectées permettront la détection des intrusions et des anomalies (via des modules intelligents à implémenter).
- Installer et configurer les modules d'un SIEMS (Security-Onion) pour l'analyse des logs collectés.

Sécurité du réseau

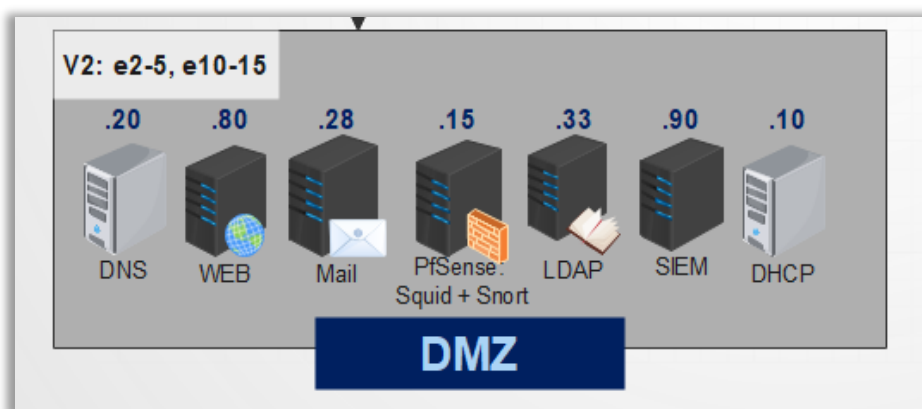
2.1 Configuration SQUID

2.1.1 Définition

Un serveur Squid est un serveur mandataire et un mandataire inverse conçu pour relayer les protocoles FTP, HTTP, Gopher, et HTTPS. Contrairement aux serveurs proxy classiques, un serveur Squid gère toutes les requêtes en un seul processus d'entrée/sortie asynchrone.

2.1.2 Configuration

Afin de configurer Squid, nous avons choisi de l'installer dans PfSense et l'implémenter dans la DMZ interne.



D'abord, on installe et on configure Pfsense dans une virtuelle machine

```
php-fpm[3741]: /system_advanced_admin.php: Successful login for user 'admin' from
: 10.0.2.12 (Local Database)

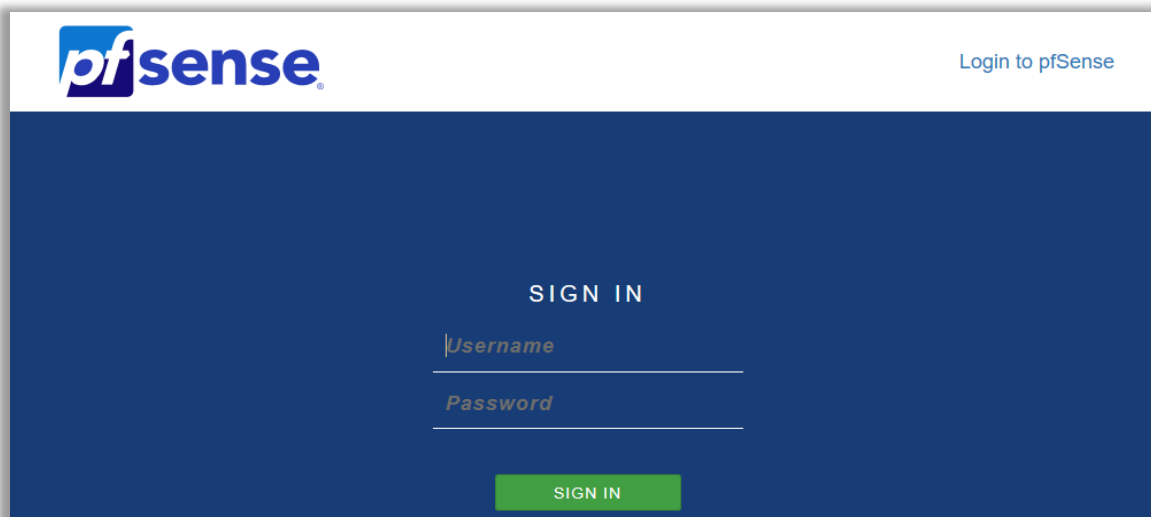
FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)
VMware Virtual Machine - Netgate Device ID: 3fa14e22b63857887886
*** Welcome to pfSense 2.6.0-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 10.0.2.38/24
LAN (lan)      -> em1      -> v4: 10.0.2.25/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults  13) Update from console
5) Reboot system              14) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell

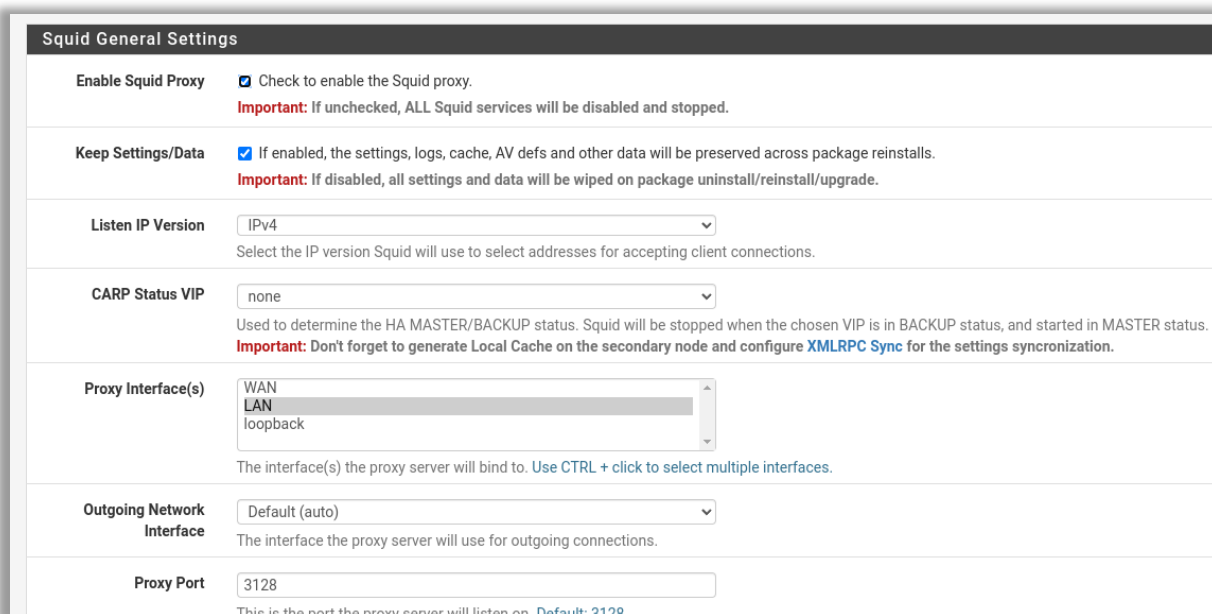
Enter an option: █
```

Après configuration des deux interfaces réseaux, on accède à l'interface graphique depuis le navigateur







Ensuite, on installe et on configure le package Squid

- Création d'une certificat DemoCA
- Activation proxy dans l'interface LAN
- Transparence du Proxy
- Port : 3128
- SSL Interception: signifie couche des sockets sécurisés (Secure Sockets Layer). Protocole pour navigateurs Web et serveurs qui permet l'authentification, le chiffrement et le déchiffrement des données envoyées sur Internet.

The image shows the "Squid General Settings" configuration page in pfSense. The page has a dark header with the title "Squid General Settings". Below the header, there are several settings sections:

- Enable Squid Proxy**: A checkbox is checked. Below it, a red "Important" note states: "If unchecked, ALL Squid services will be disabled and stopped."
- Keep Settings/Data**: A checkbox is checked. Below it, a red "Important" note states: "If disabled, all settings and data will be wiped on package uninstall/reinstall/upgrade."
- Listen IP Version**: A dropdown menu is set to "IPv4". Below it, a note says: "Select the IP version Squid will use to select addresses for accepting client connections."
- CARP Status VIP**: A dropdown menu is set to "none". Below it, a note says: "Used to determine the HA MASTER/BACKUP status. Squid will be stopped when the chosen VIP is in BACKUP status, and started in MASTER status. Important: Don't forget to generate Local Cache on the secondary node and configure XMLRPC Sync for the settings synchronization."
- Proxy Interface(s)**: A multi-select dropdown menu has "WAN" and "LAN" selected. Below it, a note says: "The interface(s) the proxy server will bind to. Use CTRL + click to select multiple interfaces."
- Outgoing Network Interface**: A dropdown menu is set to "Default (auto)". Below it, a note says: "The interface the proxy server will use for outgoing connections."
- Proxy Port**: A text input field contains "3128". Below it, a note says: "This is the port the proxy server will listen on. Default: 3128"

Transparent Proxy Settings	
Transparent HTTP Proxy	<input checked="" type="checkbox"/> Enable transparent mode to forward all requests for destination port 80 to the proxy server.  Transparent proxy mode works without any additional configuration being necessary on clients. Important: Transparent mode will filter SSL (port 443) if you enable 'HTTPS/SSL Interception' below. Hint: In order to proxy both HTTP and HTTPS protocols without intercepting SSL connections , configure WPAD/PAC options on your DNS/DHCP servers.
Transparent Proxy Interface(s)	<div> <div>WAN</div> <div>LAN</div> </div> <p>The interface(s) the proxy server will transparently intercept requests on. Use CTRL + click to select multiple interfaces.</p>
Bypass Proxy for Private Address Destination	<input type="checkbox"/> Do not forward traffic to Private Address Space (RFC 1918 and IPv6 ULA) destinations. Destinations in Private Address Space (RFC 1918 and IPv6 ULA) are passed directly through the firewall, not through the proxy server.
Bypass Proxy for These Source IPs	<input type="text"/> <p>Do not forward traffic from these source IPs, CIDR nets, hostnames, or aliases through the proxy server but let it pass directly through the firewall. Applies only to transparent mode. Separate entries by semi-colons (;)</p>
Bypass Proxy for These Destination IPs	<input type="text"/> <p>Do not proxy traffic going to these destination IPs, CIDR nets, hostnames, or aliases, but let it pass directly through the firewall. Applies only to transparent mode. Separate entries by semi-colons (;)</p>

SSL Man In the Middle Filtering	
HTTPS/SSL Interception	<input checked="" type="checkbox"/> Enable SSL filtering.
SSL/MITM Mode	<div>Splice All</div> <p>The SSL/MITM mode determines how SSL interception is treated when 'SSL Man In the Middle Filtering' is enabled. Default: Splice Whitelist, Bump Otherwise. Click Info for details. </p>
SSL Intercept Interface(s)	<div> <div>WAN</div> <div>LAN</div> </div> <p>The interface(s) the proxy server will intercept SSL requests on. Use CTRL + click to select multiple interfaces.</p>
SSL Proxy Port	<div>3129</div> <p>This is the port the proxy server will listen on to intercept SSL while using transparent proxy. Default: 3129</p>
SSL Proxy Compatibility Mode	<div>Modern</div> <p>The compatibility mode determines which cipher suites and TLS versions are supported. Default: Modern. Click Info for details. </p>
DHParams Key Size	<div>2048 (default)</div> <p>DH parameters are used for temporary/ephemeral DH key exchanges and improve security by enabling the use of DHE ciphers.</p>
CA	<div>DemoCA</div> <p>Select Certificate Authority to use when SSL interception is enabled. </p>

Headers Handling, Language and Other Customizations	
Visible Hostname	<div>squid.sysco.ma</div> <p>This is the hostname to be displayed in proxy server error messages.</p>
Administrator's Email	<div>bentaja@sysco.ma</div> <p>This is the email address displayed in error messages to the users.</p>

Enfin, on active le filtrage par SquidGuard

General Options

Enable ☒ Check this option to enable squidGuard.

Important: Please set up at least one category on the 'Target Categories' tab before enabling. See [this link for details](#).
The Save button at the bottom of this page must be clicked to save configuration changes.
To activate squidGuard configuration changes, **the Apply button must be clicked**.

SquidGuard service state: **STARTED**

LDAP Options

- Téléchargement des listes de filtrage

Blacklist Update

0 %

Enter FTP or HTTP path to the blacklist archive here.

- Création d'un ACL

General Options

Name

Enter a unique name of this rule here.
The name must consist between 2 and 15 symbols [a-Z_0-9]. The first one must be a letter.

Order

Select the new position for this target category. Target categories are listed in this order on ACLs and are matched from the top down in sequence.

Domain List

General Options

Disabled ☐ Check this to disable this ACL rule.

Name

Enter a unique name of this rule here.
The name must consist between 2 and 15 symbols [a-Z_0-9]. The first one must be a letter.

Order

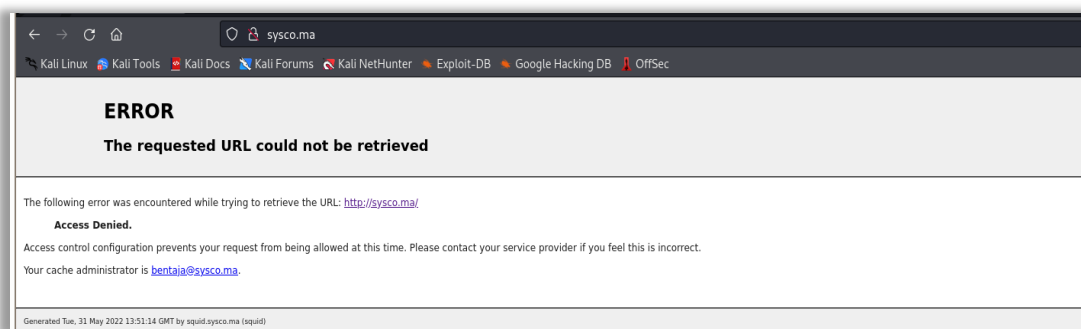
Select the new position for this ACL item. ACLs are evaluated on a first-match source basis.
Note: Search for a suitable ACL by field 'source' will occur before the first match. If you want to define an exception for some sources (IP) from the IP range, put them on first of the list.
Example: ACL with single (or short range) source ip 10.0.0.15 must be placed before ACL with more large ip range 10.0.0.0/24.

Client (source)

- Bloquer notre nom de domaine pour vérifier le fonctionnement de notre proxy



- Vérification



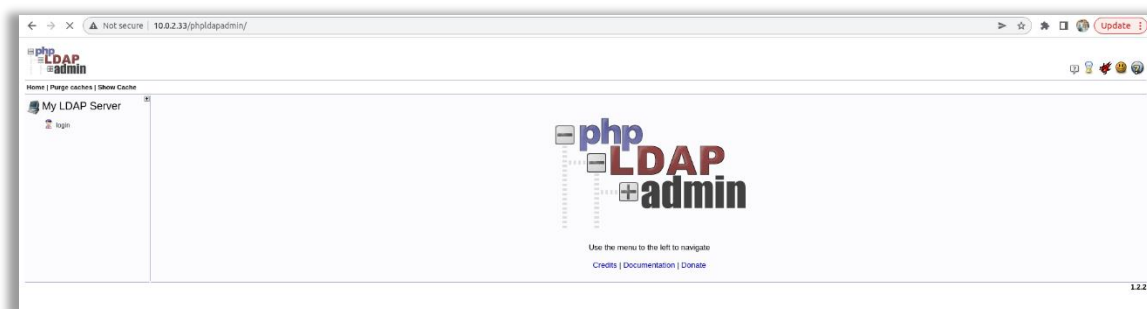
2.2 Configuration OPENLDAP

2.2.1 Définition

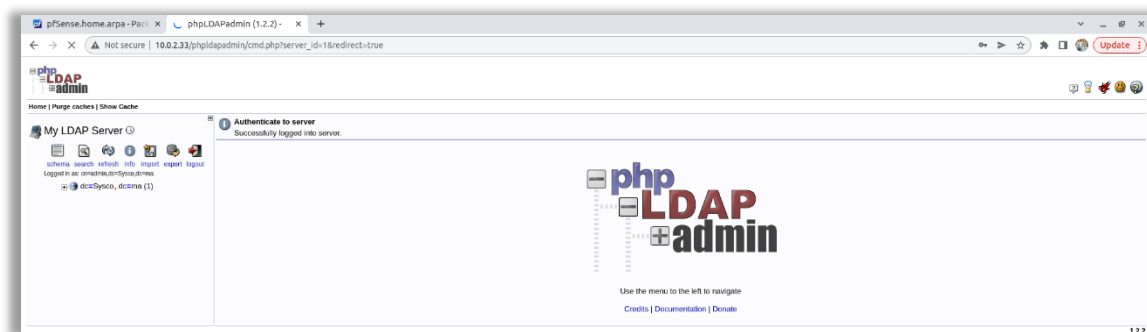
OpenLDAP est un annuaire informatique qui fonctionne sur le modèle client/serveur. Il contient des informations de n'importe quelle nature qui sont rangées de manière hiérarchique.

2.2.2 Configuration LDAP

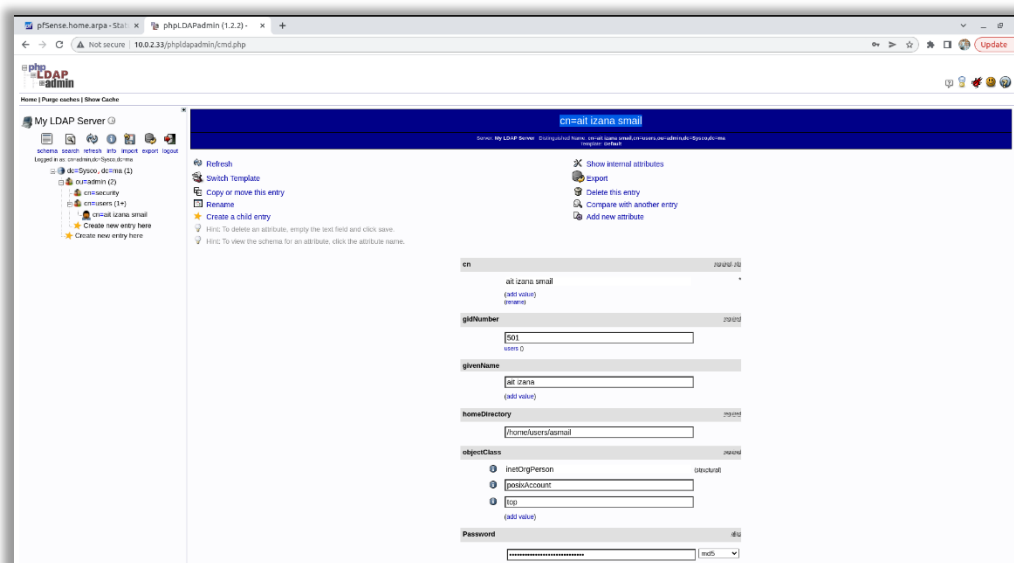
On va d'abord installer le serveur Openldap sur notre machine, et puis le lier avec le SQUID, pour permettre l'authentification à partir du l'annuaire.



Après authentification, on accède à l'interface graphique d'accueil



On crée un utilisateur dans LDAP pour s'authentifier



On configure l'authentification du squid par ldap

Squid Authentication General Settings	
Authentication Method	LDAP <small>Select an authentication method. This will allow users to be authenticated by local or external services.</small>
Authentication Server	10.0.2.33 <small>Enter the IP or hostname of the server that will perform the authentication here.</small>
Authentication server port	389 <small>Enter the port to use to connect to the authentication server here. Leave this field blank to use the authentication method's default port.</small>

On ajoute le chemin de l'utilisateur

The screenshot shows the 'Squid Authentication LDAP Settings' window. It contains the following fields and options:

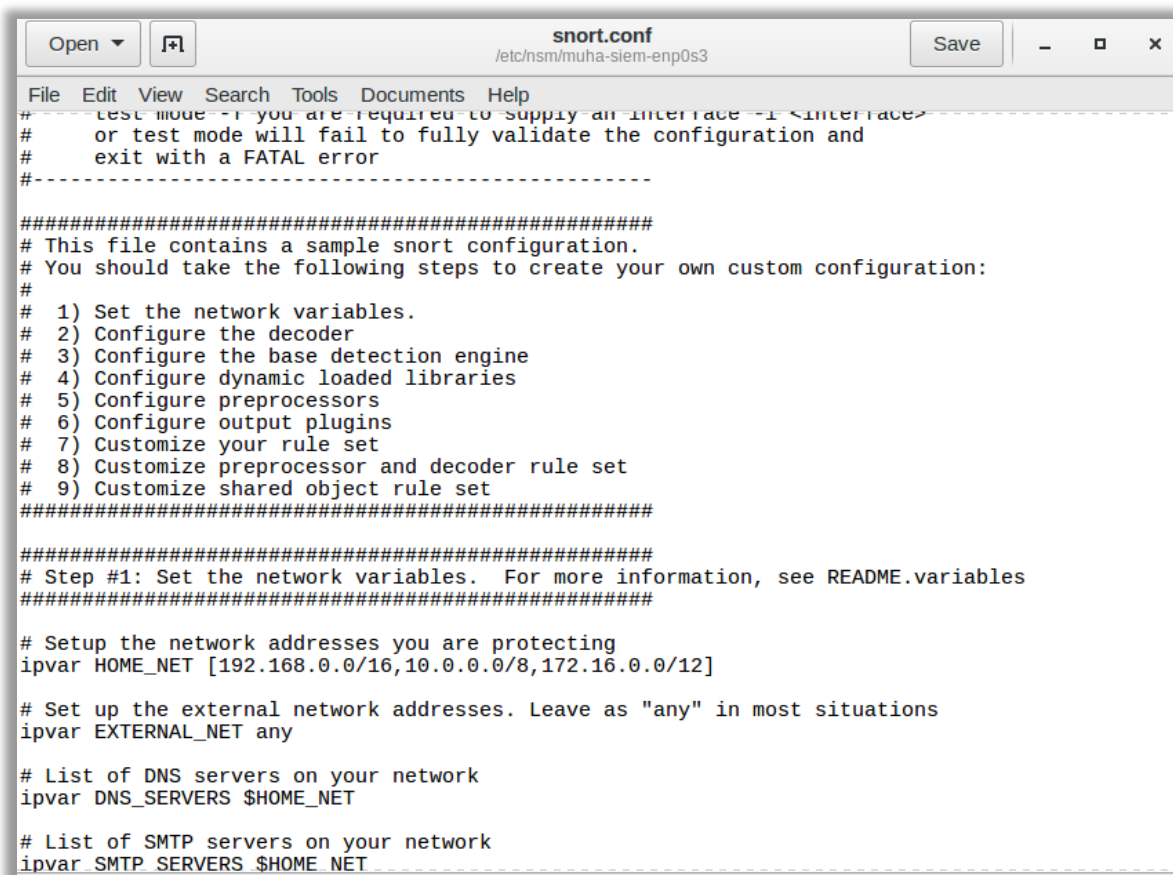
- LDAP version:** A dropdown menu set to '3'. Below it, the text 'Select LDAP protocol version.' is displayed.
- Transport:** A dropdown menu set to 'TCP - Standard'. Below it, a note states: 'If 'SSL Encrypted' or 'TCP - STARTTLS' is selected, the CA certificate of the LDAP server must be trusted by the Operating System Trust Store. This is automatic for certificates signed by globally trusted CAs such as Let's Encrypt; self-signed CAs can optionally be added to the Trust Store on pfSense 2.5.'
- LDAP Server User DN:** A text input field containing 'cn=ait izana smail,cn=users,ou=admin,dc=Sysco,dc=ma'. Below it, the text 'Enter the user DN to use to connect to the LDAP server here.' is displayed.
- LDAP Password:** A text input field with masked characters '....'. Below it, the text 'Enter the password to use to connect to the LDAP server here.' is displayed.
- LDAP Base Domain:** A text input field containing 'dc=Sysco,dc=ma'. Below it, the text 'Enter the base domain of the LDAP server here.' is displayed.
- LDAP Username DN Attribute:** A text input field containing 'uid'. Below it, the text 'Enter LDAP username DN attribute here.' is displayed.
- LDAP Search Filter:** A text input field containing '(&(objectClass=person)(uid=%s))'. Below it, the text 'Enter LDAP search filter here.' is displayed.
- LDAP not follow referrals:** A checkbox labeled 'Do not follow referrals.' which is currently unchecked.

2.3 Configuration Snort IDS

Pour le l'IDS, on a choisi d'utiliser l'IDS de security onion.

On a utilisé l'outil sgul offert par security onion, qui est construit par des analystes de sécurité réseau pour des analystes de sécurité réseau. Le composant principal de Sguil est une interface graphique intuitive qui permet d'accéder aux événements en temps réel, aux données de session et aux captures de paquets bruts. Sguil facilite la pratique de la surveillance de la sécurité du réseau et de l'analyse événementielle.

Et voici notre fichier de configuration :



```
File Edit View Search Tools Documents Help
#-----test mode-----If you are required to supply an interface -I <interface>
# or test mode will fail to fully validate the configuration and
# exit with a FATAL error
#-----
#####
# This file contains a sample snort configuration.
# You should take the following steps to create your own custom configuration:
#
# 1) Set the network variables.
# 2) Configure the decoder
# 3) Configure the base detection engine
# 4) Configure dynamic loaded libraries
# 5) Configure preprocessors
# 6) Configure output plugins
# 7) Customize your rule set
# 8) Customize preprocessor and decoder rule set
# 9) Customize shared object rule set
#####
#####
# Step #1: Set the network variables. For more information, see README.variables
#####
# Setup the network addresses you are protecting
ipvar HOME_NET [192.168.0.0/16,10.0.0.0/8,172.16.0.0/12]
# Set up the external network addresses. Leave as "any" in most situations
ipvar EXTERNAL_NET any
# List of DNS servers on your network
ipvar DNS_SERVERS $HOME_NET
# List of SMTP servers on your network
ipvar SMTP_SERVERS $HOME_NET
```

HOME_NET: Cette variable définit l'adresse du réseau interne que vous souhaitez protéger.

EXTERNAL_NET: Cette variable définit le réseau externe que vous avez l'intention de surveiller.

Et on a testé notre réseau par l'outil nmap et notre IDS a détecté cette activité :

The screenshot shows the SGUIL-0.9.0 interface. The top bar indicates 'Connected To localhost' and the date/time is '2022-06-01 10:03:08 GMT'. The main window displays a list of 'RealTime Events' with columns: ST, Sensor, Alert ID, Date/Time, Src IP, SPort, Dst IP, DPort, Pr, and Event Message. Below the list, there are tabs for 'IP Resolution', 'Agent Status', 'Snort Statistics', and 'System Msg'. The 'System Msg' tab is active, showing a packet analysis window with fields for Source IP, Destination IP, Source Port, Destination Port, and various protocol details like UAPRSF, Seq #, Ack #, and Window. The packet analysis window also includes a 'Search Packet Payload' field and radio buttons for 'Hex', 'Text', and 'NoCase'.

ST	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	muha-sie...	3.13	2022-06-01 09:22:57	10.0.2.45	56094	10.0.2.28	80	6	ET SCAN Nmap Scripting En...
RT	muha-sie...	3.14	2022-06-01 09:22:57	10.0.2.45	56094	10.0.2.28	80	6	ET SCAN Possible Nmap Us...
RT	muha-sie...	3.195	2022-06-01 09:33:28	10.0.2.45		10.0.2.80		1	GPL ICMP_INFO PING *NIX
RT	muha-sie...	3.129	2022-06-01 09:29:37	10.0.2.80	80	10.0.2.45	48162	6	GPL WEB_SERVER 403 For...
RT	muha-sie...	3.23	2022-06-01 09:22:57	10.0.2.28	80	10.0.2.45	56094	6	GPL WEB_SERVER 403 For...
RT	muha-sie...	1.1	2022-06-01 09:16:41	0.0.0.0		0.0.0.0			[OSSEC] Integrity checksum...
RT	muha-sie...	3.1	2022-06-01 09:19:39	10.0.2.45	68	10.0.2.23	67	17	ET POLICY Possible Kali Lin...
RT	muha-sie...	1.12	2022-06-01 09:17:08	0.0.0.0		0.0.0.0			[OSSEC] New group added t...
RT	muha-sie...	1.13	2022-06-01 09:17:10	0.0.0.0		0.0.0.0			[OSSEC] New user added to ...
RT	muha-sie...	3.2	2022-06-01 09:22:45	10.0.2.45	51754	10.0.2.28	3306	6	ET SCAN Suspicious inbound...
RT	muha-sie...	3.6	2022-06-01 09:22:48	10.0.2.45	47956	10.0.2.28	5432	6	ET SCAN Suspicious inbound...
RT	muha-sie...	3.8	2022-06-01 09:22:48	10.0.2.45	59836	10.0.2.28	1521	6	ET SCAN Suspicious inbound...
RT	muha-sie...	3.11	2022-06-01 09:22:50	10.0.2.45	52390	10.0.2.28	1433	6	ET SCAN Suspicious inbound...

Et pour voir les évènements reliés à un évènement :

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	5	muha-sie...	3.2	2022-06-01 09:22:45	10.0.2.45	51754	10.0.2.28	3306	6	ET SCAN Suspicious inbound...
RT	3	muha-sie...	3.5	2022-06-01 09:22:47	10.0.2.45	51598	10.0.2.28	5904	6	ET SCAN Potential VNC Sca...
RT	4	muha-sie...	3.6	2022-06-01 09:22:48	10.0.2.45	47956	10.0.2.28	5432	6	ET SCAN Suspicious inbound...
RT	4	muha-sie...	3.8	2022-06-01 09:22:48	10.0.2.45	59836	10.0.2.28	1521	6	ET SCAN Suspicious inbound...
RT	3	muha-sie...	3.10	2022-06-01 09:22:49	10.0.2.45	50118	10.0.2.28	5811	6	ET SCAN Potential VNC Sca...
RT	4	muha-sie...	3.11	2022-06-01 09:22:50	10.0.2.45	52390	10.0.2.28	1433	6	ET SCAN Suspicious inbound...
RT	87	muha-sie...	3.13	2022-06-01 09:22:57	10.0.2.45	56094	10.0.2.28	80	6	ET SCAN Nmap Scripting En...
RT		View Correlated Events	3.14	2022-06-01 09:22:57	10.0.2.45	56094	10.0.2.28	80	6	ET SCAN Possible Nmap Us...
RT	31	muha-sie...	3.23	2022-06-01 09:22:57	10.0.2.28	80	10.0.2.45	56094	6	GPL WEB_SERVER 403 For...
RT	1	muha-sie...	1.27	2022-06-01 09:23:34	0.0.0.0		0.0.0.0		0	[OSSEC] Web server 400 err...
RT	1	muha-sie...	1.28	2022-06-01 09:26:03	0.0.0.0		0.0.0.0		0	[OSSEC] Received 0 packet...
RT	60	muha-sie...	3.129	2022-06-01 09:29:37	10.0.2.80	80	10.0.2.45	48162	6	GPL WEB_SERVER 403 For...
RT	46	muha-sie...	3.195	2022-06-01 09:33:28	10.0.2.45		10.0.2.80		1	GPL ICMP_INFO PING *NIX

RT	1	muha-sie...	3.13	2022-06-01 09:22:57	10.0.2.45	56094	10.0.2.28	80	6	ET SCAN Nmap Scripting Engi...
RT	1	muha-sie...	3.15	2022-06-01 09:22:57	10.0.2.45	56098	10.0.2.28	80	6	ET SCAN Nmap Scripting Engi...
RT	1	muha-sie...	3.17	2022-06-01 09:22:57	10.0.2.45	56104	10.0.2.28	80	6	ET SCAN Nmap Scripting Engi...
RT	1	muha-sie...	3.19	2022-06-01 09:22:57	10.0.2.45	56108	10.0.2.28	80	6	ET SCAN Nmap Scripting Engi...
RT	1	muha-sie...	3.21	2022-06-01 09:22:57	10.0.2.45	56110	10.0.2.28	80	6	ET SCAN Nmap Scripting Engi...
RT	1	muha-sie...	3.24	2022-06-01 09:22:57	10.0.2.45	56114	10.0.2.28	80	6	ET SCAN Nmap Scripting Engi...
RT	1	muha-sie...	3.26	2022-06-01 09:22:57	10.0.2.45	56116	10.0.2.28	80	6	ET SCAN Nmap Scripting Engi...
RT	1	muha-sie...	3.28	2022-06-01 09:22:57	10.0.2.45	56118	10.0.2.28	80	6	ET SCAN Nmap Scripting Engi...
RT	1	muha-sie...	3.30	2022-06-01 09:22:57	10.0.2.45	56120	10.0.2.28	80	6	ET SCAN Nmap Scripting Engi...
RT	1	muha-sie...	3.32	2022-06-01 09:22:57	10.0.2.45	56122	10.0.2.28	80	6	ET SCAN Nmap Scripting Engi...
RT	1	muha-sie...	3.34	2022-06-01 09:22:57	10.0.2.45	56126	10.0.2.28	80	6	ET SCAN Nmap Scripting Engi...
RT	1	muha-sie...	3.46	2022-06-01 09:22:57	10.0.2.45	56130	10.0.2.28	80	6	ET SCAN Nmap Scripting Engi...

Et maintenant on a consulter les logs de notre routeur R3.

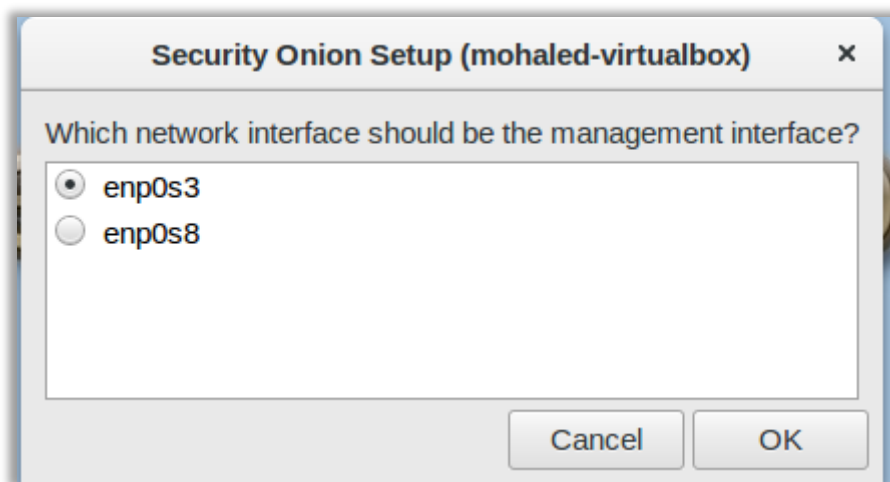
Dans le fichier 10.log on voit que l'interface serial0/0 a changé à l'état down (on a débranché cette interface)

```
[root@selcentos1 okio]# ls /var/log/REMOTELOGS/10.0.4.1/
10.log 12.log 14.log 16.log 18.log 1.log 21.log 23.log 3.log 5.log 7.log 9.log
11.log 13.log 15.log 17.log 19.log 20.log 22.log 2.log 4.log 6.log 8.log
[root@selcentos1 okio]# tail /var/log/REMOTELOGS/10.0.4.1/10.log
2022-05-31T13:56:09.303706+01:00 10.0.4.1 22: *May 31 11:54:26.751: %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 10.0.2.90 port 514 started - CLI initiated
[root@selcentos1 okio]# tail /var/log/REMOTELOGS/10.0.4.1/11.log
2022-06-01T09:20:06.526396+01:00 10.0.4.1 1: *Mar 1 00:00:10.263: %IOS_LICENSE_IMAGE_APPLICATION-6-LICENSE_LEVEL: Module name = c2900 Next reboot level = ipbasek9 and License = ipbasek9
[root@selcentos1 okio]# tail /var/log/REMOTELOGS/10.0.4.1/10.log
2022-06-01T09:20:06.526396+01:00 10.0.4.1 10: *Jun 1 07:18:12.843: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1, changed state to down
[root@selcentos1 okio]#
```

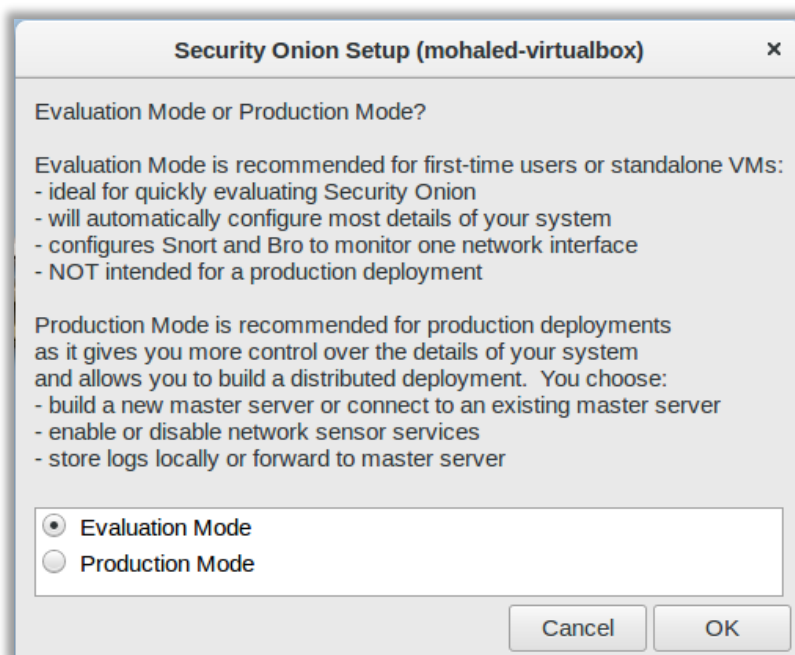
2.5 Configuration SIEM

Pour l'implémentation de notre SIEM, on a utilisé security onion qui est une distribution Linux gratuite et open source préparée pour la détection des intrusions, la surveillance de la sécurité et la gestion des journaux à l'aide d'outils de sécurité, à savoir Snort, Suricata, Sguil, Squert, NetworkMiner et Kibana, comme indiqué par Security Onion.

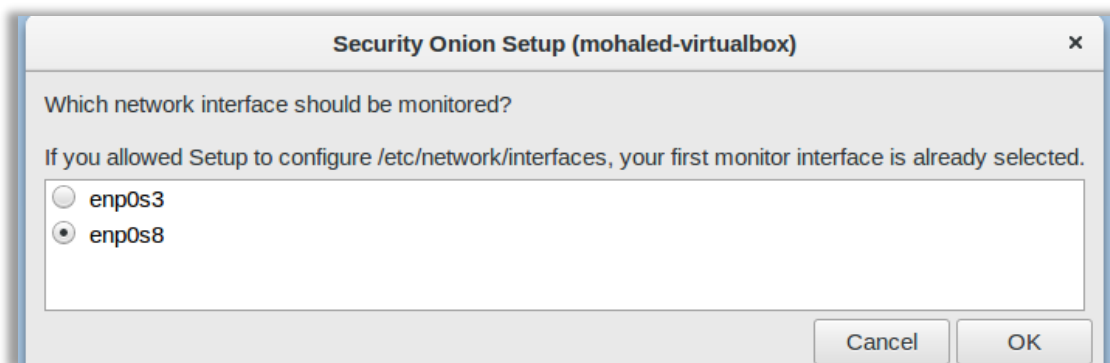
Configuration d'interface de Sniffing :



Pour le mode d'utilisation on a opté pour un mode d'évaluation :

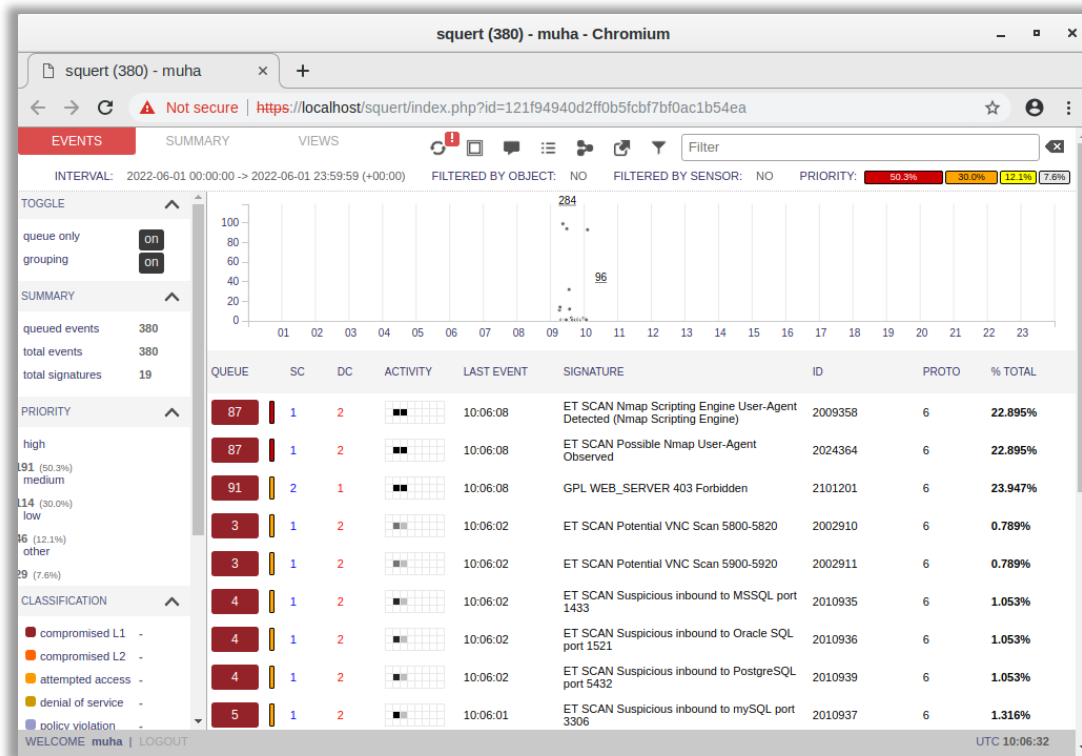


Et on a configuré l'interface de monitoring :



Une fois l'installation s'est terminé on a essayé de scanner l'adresse ip d'une machine au sein de notre réseau en utilisant nmap :

Des alerts sont affichés sur l'interface quiert de notre siem security onion :



Aussi si on fait beaucoup des pings sur une machine donné au sein de notre réseau d'entreprise ils s'affichent dans squier

